tufin The Security Policy Company. + aws

Informe de solución conjunta

Visibilidad, cumplimiento normativo y automatización para Amazon Web Services (AWS)

Ventajas para su empresa:

- Mayor visibilidad de la seguridad en AWS y en toda la red heterogénea.
- Aumento de la agilidad gracias a una coordinación de políticas de seguridad que abarca tanto el Cloud como las infraestructuras on-premise.
- Automatización de las operaciones de seguridad de modo que AWS establezca controles integrados.
- Garantía de una segmentación y cumplimiento de políticas estrictos en AWS y en toda la red híbrida.
- Reducción de los tiempos de preparación de auditorías hasta en un 70% gracias al cumplimiento normativo continuo.
- Solución de problemas y proporcionar conectividad para aplicaciones a través de la red.

La incorporación del Cloud está creciendo en todas las geografías e industrias, y AWS ha recibido la calificación de líder en el mercado IaaS (infraestructura como servicio)1. La mayoría de las empresas está utilizando o planificando utilizar AWS para agilizar la disponibilidad de nuevos servicios y aplicaciones a los clientes[2].

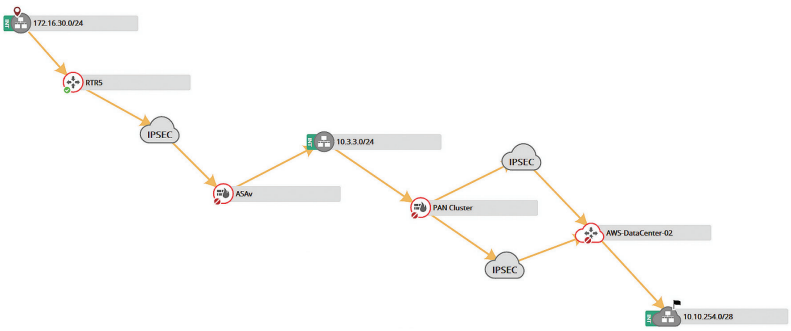
Aunque muchas empresas alojan nuevas aplicaciones en AWS o migran aplicaciones existentes, todavía existen muchas dudas acerca de la definición y aplicación de las políticas de seguridad en AWS. A fin de evitar retrasos y obtener la agilidad óptima que AWS ofrece, los equipos de seguridad no suelen participar en los cambios diarios en la seguridad y conectividad de AWS ni en la configuración inicial de los grupos de seguridad de AWS.

Además de los retos de visibilidad y aplicación en AWS, la mayoría de las empresas que comienzan a utilizar AWS, todavía disponen de infraestructuras físicas y virtuales que seguirán administrando. Estos entornos heterogéneos de Cloud pública, Cloud privada y redes físicas plantean retos de visibilidad, seguridad y conectividad entre proveedores y plataformas, y pueden poner en riesgo de forma significativa la seguridad, el cumplimiento normativo e incluso la disponibilidad de aplicaciones críticas.

Visibilidad centralizada en AWS y redes locales

La visibilidad es fundamental para gestionar la seguridad y la conectividad en redes aunque estas sean heterogéneas. Los equipos de operaciones de seguridad y red que no disponen de visibilidad de los grupos y las reglas de seguridad de AWS no pueden identificar los incumplimientos de políticas ni prepararse para auditorías. Con Tufin, pueden realizar el descubrimiento automático de instancias de AWS, así como de aplicaciones y conectividad de las mismas, etiquetas, grupos y reglas de seguridad, y mantenerse actualizados gracias a la supervisión de cambios en tiempo real. En función de esta visibilidad, también pueden realizar análisis para identificar violaciones de la política de seguridad de la organización o la normativa del sector.

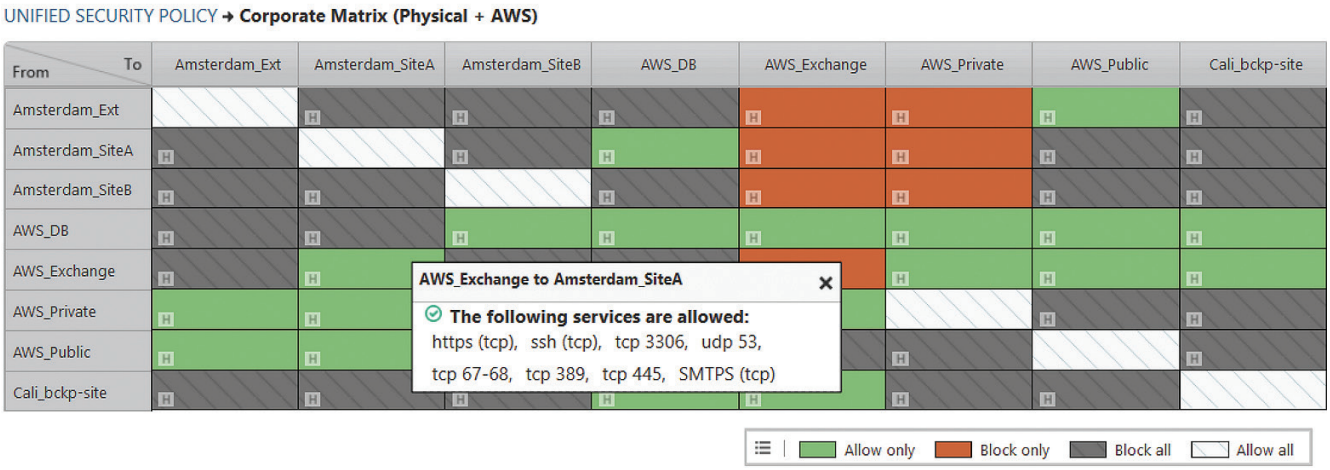
Además, el uso de varias plataformas y proveedores en la red híbrida dificulta, en gran medida, la visualización de la conectividad para las aplicaciones que comprenden tanto AWS como las infraestructuras on-premise. Mediante la gestión centralizada de las plataformas de Cloud públicas y privadas, así como de routers y firewalls físicos, Tufin proporciona una visualización de la conectividad de las aplicaciones que puede utilizarse para solucionar fallos o planificar cambios y migraciones.



análisis interactivo de rutas de topología de Tufin permite visualizar la conectividad en firewalls locales y de AWS

Cumplimiento de políticas y preparación para auditorías en aplicaciones de AWS

Los controles de seguridad y cumplimiento normativo que se definen y aplican en las instalaciones locales, y habitualmente, no se aplican en las plataformas de Cloud. Sin embargo, las aplicaciones alojadas en AWS deben adaptarse a las políticas de la organización con el fin de proteger sistemas y datos sensibles y hacer frente al siguiente ciberataque. Tufin ayuda a sus clientes a definir y aplicar la Política Unificada de Seguridad (Unified Security Policy™) de forma centralizada, lo que permite reforzar la segmentación de la red y aplicar un cumplimiento normativo continuo de los estándares internos y del sector, tales como PCI DSS, GPDR, SOX, HIPAA, NERC CIP e ISO 27001. Mediante la aplicación del cumplimiento normativo continuo, las organizaciones no solo evitan las sanciones asociadas al incumplimiento, sino que también pueden reducir la carga de trabajo de preparación para auditorías hasta en un 70%. Los equipos de seguridad pueden evitar la falta de comunicación con los equipos del Cloud mediante la adopción de un control integrado de políticas de seguridad que no retrase la entrega de nuevas aplicaciones y servicios.



La Política Unificada de Seguridad (Unified Security Policy™) de Tufin aplica segmentación de una zona a otra en AWS y la red híbrida

Aumento de la agilidad gracias a la automatización completa

La agilidad es el factor clave y más critico en lo que a competitividad se refiere siendo el más importante en el panorama empresarial actual. Sin embargo, para las aplicaciones verticales que utilizan AWS y las infraestructuras locales, la agilidad puede verse limitada debido a la disparidad de los sistemas de gestión y orquestación. Una aplicación puede estar completamente implementada en AWS, pero debe esperar para obtener acceso a una base de datos del centro de datos a través de firewalls y routers físicos antes de ponerse en marcha. Mediante la gestión centralizada y el proceso de cambios totalmente automatizado de Tufin, los clientes pueden implementar los requisitos de conectividad de un extremo a otro en toda la red aunque esta sea hetereogénea.

El proceso de cambio proporcionado por Tufin incluye un análisis de riesgos automatizado para un cumplimiento de políticas integrado, un diseño automatizado y una implementación para firewalls y plataformas de Cloud, así como una verificación automatizada que permite aumentar la productividad y acelerar la puesta en producción.

Tufin proporciona una implementación automatizada de cambios en los grupos de seguridad de AWS y ayuda a los usuarios a identificar el grupo de seguridad adecuado que debe modificarse. Tufin se basa en la orquestación de extremo a extremo y proporciona también un proceso automatizado para la migración de aplicaciones a AWS. El modelo de conectividad de una aplicación se puede duplicar e implementar en AWS con una interfaz de usuario basada en asistentes y, a continuación, la aplicación original puede retirarse del servicio con el proceso de Tufin lo que incrementa la seguridad de la red.

Tufin® es el líder en mercado en Orquestación de Políticas de Seguridad, atendiendo a más de la mitad de las 50 principales compañías de Forbes Global 2000. Tufin simplifica la administración de algunas de las redes más grandes y complejas del mundo, que consisten en miles de firewalls, dispositivos de red y emergentes infraestructuras de cloud híbrida. Las empresas eligen la galardonada Tufin Orchestration Suite™ para para aumentar la agilidad frente a la gran demanda de cambios en el negocio, a la vez que mantienen una sólida postura de seguridad Tufin reduce la superficie de ataque y satisface la necesidad de una mayor visibilidad de la conectividad de aplicaciones de forma segura y confiable. Su automatización de seguridad de red permite a las empresas implementar cambios en minutos con análisis de riesgo pro-activo y cumplimiento continuo de políticas. Tufin da servicio a más de 2,100 clientes que abarcan todas las industrias y áreas geografías; sus productos y tecnologías están protegidos por patente en los EE. UU. y en otros países Más información en **www.tufin.com.**

1 Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide report, Lydia Leong et al., publicado el 3 de agosto de 2016
2 State Of The Cloud Report de RightScale de 2016